

Vol. 12 (1), Abril 2014, 427-441

ISSN: 1887-4592

Fecha de recepción: 14-03-2013

Fecha de aceptación: 03-08-2013

## **Criptored y las redes temáticas orientadas a la educación global.**

**Alfonso Muñoz Muñoz**  
**Jorge Ramío Aguirre**

Universidad Politécnica de Madrid  
Escuela Universitaria de Informática  
España

## **Criptored and the thematic networks oriented to global education.**

**Alfonso Muñoz Muñoz**  
**Jorge Ramío Aguirre**

Universidad Politécnica de Madrid  
Escuela Universitaria de Informática  
Spain

### **Resumen**

La presente investigación recoge una experiencia de innovación educativa de 13 años de duración que analiza las bondades e inconvenientes de utilizar redes temáticas orientadas a la educación de la ciudadanía. Esta experiencia se centra en la red temática Criptored fundada en 1999 en la Universidad Politécnica de Madrid. La experiencia publicada en este trabajo demuestra que una red temática puede ser no sólo un buen medio para difundir conocimiento de calidad entre especialistas, sino un buen generador de ideas y proyectos derivados con implicaciones formativas directas de la ciudadanía a través de Internet. Esta demostración se fundamenta en una serie de diferen-

### **Abstract**

This research describes a 13-years-long educational and innovative experience which analyzes the advantages and disadvantages of using thematic networks with educational purposes. The above mentioned experience sets the spotlight on the thematic network Criptored, which was founded in 1999 at the Technical University of Madrid. The experience published on this work proves that a thematic network can be not only a good way to spread awareness of quality among specialists but also a good generator of ideas and projects arising with direct educational implications for people's learning through Internet. This demonstration is based on several different decisions made

tes decisiones en la evolución de este proyecto, como son una estructuración docente de la información publicada, gestión de la calidad de los contenidos, definición de un esquema de difusión y compartición de información, generación de nuevo contenido basado en interacciones de miembros y no miembros de la red, etc., lo que facilita la apertura de una red temática a un público heterogéneo sin perder calidad ni excelencia. El impacto y la difusión de esta red en diversos sectores quedan retratados por los resultados. La red refleja un impacto significativo en universidades, centros de investigación, empresas TIC en España e Iberoamérica y en la sociedad en general: 243 universidades, centros de investigación y asociaciones de 22 países representados, 925 miembros de la red, 448 documentos para libre descarga, 14 libros electrónicos, 102 vídeos y más de 2.500.000 documentos servidos en 13 años.

**Palabras clave:** : educativa, formación online, redes temáticas, Criptored, seguridad de la información.

along the evolution of this project, such as a teaching structure of the information published, content quality management, the creation of brand new content based on both members and non-members of the network and so on. All these features ease the opening of a new thematic network to a heterogeneous target public without detriment to either quality or excellence. The impact and broadcasting of this network in many sectors clearly match its results. In fact, the network shows meaningful impact on universities, research centers, technology and information communications companies in Spain and Latin America, as well as society in general: 243 universities, research centers and associations from 22 countries, 925 network members, 448 free downloadable documents, 14 electronic books, 102 videos, more than 2.500.000 documents delivered in 13 years, etc.

**Key words:** educational innovation, e-learning, thematic networks, Criptored, information security.

## Introducción a las redes temáticas

En los inicios de Internet la única forma de aprendizaje a través de una red telemática era la obtención de contenidos accesibles desde otra entidad de la red. El problema residía en cómo encontrar esos contenidos ya que no existían fuentes de recomendación adecuadas. Este problema creció con el éxito de los sitios Web, de forma que comenzaban a existir recursos de utilidad pero difícilmente accesibles. Los buscadores mejoraron la situación, si bien la dispersión y falta de cooperación entre los distintos sitios plantean problemas de repetición de contenidos, coherencia entre distintas visiones de un mismo tema, etc. Las comunidades virtuales vinieron a dar una solución a este problema. Según Howard Rheingold creador del término comunidad virtual (Rheingold, 1993), las comunidades virtuales son herramientas con fines determinados. Este enfoque habilita la idea de utilizar las comunidades virtuales como herramientas de transmisión de conocimiento con estructuras académicas y docentes.

Una comunidad virtual es un concepto abstracto que debe materializarse en aplicaciones. En los últimos años han surgido distintas aplicaciones orientadas a la creación de este tipo de comunidades. Entre las más recientes y exitosas, especialmente desde un punto de vista académico y docente, se pueden destacar los servicios basados en las redes sociales, los blogs, foros, wikis, cursos online y las redes temáticas. Veamos breve-

mente cada uno de ellos:

- **Servicios basados en redes sociales.** Son servicios que mediante la generación de perfiles de usuarios y normalización de conexiones entre ellos, reflejan relaciones sociales entre miembros con intereses comunes (Boyd y Ellison, 2007). Desde un punto de vista docente y formativo estos servicios pueden ofrecer gran utilidad al mezclar conceptos como la comunicación (poner en común conocimientos), la comunidad (encontrar/integrar comunidades) y la cooperación (hacer cosas juntos).
- **Blogs, foros y wikis.** Estas herramientas están siendo usadas activamente para cuestiones relacionadas con la educación. Permiten resolver cuestiones, desarrollar conceptos de forma colaborativa, facilitar una estructura de separación de distintos conceptos, etc.
- **Cursos online.** Cursos específicos sobre un tema dado. Existen multitud de variantes. Últimamente están surgiendo los llamados Massive Open Online Course (MOOC) que pretenden democratizar el acceso a una educación de calidad de la manera más sencilla posible. Muchos de sus cursos cubren materias de forma similar a como se haría en una carrera universitaria. Este tipo de cursos se está “consumiendo” por un gran número de alumnos que valoran estos recursos novedosos y gratuitos de aprendizaje (Jódar, 2013).
- **Redes temáticas.** Tradicionalmente las redes temáticas son asociaciones de grupos de investigación de entidades públicas o privadas, cuyas actividades científicas o tecnológicas están relacionadas dentro de un ámbito común de interés, con la intención de establecer interacciones científicas estables y continuadas, intercambio de conocimiento científico y técnico de mutuo interés, potenciación sinérgica y coordinación de sus líneas de I+D+i, etc.

Desde un punto de vista formativo, docente y académico, las anteriores comunidades virtuales pueden ser analizadas considerando al menos 4 características: área de conocimiento, relación entre los miembros de una comunidad, capacidad de estructuración de los contenidos y área de influencia. Una posible representación de estas características asociadas a cada comunidad virtual en particular puede verse en el gráfico 1.

	Área de conocimiento	Relaciones entre miembros de la comunidad	Capacidad de estructuración de contenidos	Área de Influencia
<b>Social Networking Services</b>	Amplio espectro	Relaciones personales-profesionales	Baja	Potencialmente alta

	Área de conocimiento	Relaciones entre miembros de la comunidad	Capacidad de estructuración de contenidos	Área de Influencia
<b>Blog (incluye, foros, wikis, etc.)</b>	Específicas	Relaciones personales o basadas en roles	Media	Potencialmente alta
<b>Online courses</b>	Específicas del curso a tratar	Relaciones basadas en roles	Muy alta	Media (excepto con los MOOC que pasa a ser potencialmente alta)
<b>Redes Temáticas</b>	Temática	Relaciones basadas en contenidos	Media/alta	Media

**Gráfico n.1.** Una posible representación de las características de cada aplicación de comunidad virtual

Todas las comunidades virtuales anteriores son de gran interés desde un punto de vista formativo y docente; no obstante, nuestra experiencia educativa se centra en un tipo concreto de ellas, las redes temáticas, y particularmente en el caso de la red temática Criptored creada en la Universidad Politécnica de Madrid. Después de 13 años de vida, es posible demostrar en esta investigación cómo una red temática (al menos de la temática que cubre esta red) puede extender sus brazos más allá de las asociaciones de investigación tradicionales entre sus miembros y convertirse en un verdadero proveedor de conocimiento global a ciudadanos de todo tipo, conocimientos de gran calidad verificados por expertos. La ventaja de esta extensión es que ciudadanos que no pertenecieran a esa red temática formalmente podrían disfrutar del conocimiento que ella genera y aporta. A continuación se profundiza en esta red temática que ha permitido observar los resultados enunciados.

## Red temática Criptored. Hipótesis y retos

Las redes temáticas son una herramienta usual para favorecer la coordinación de distintos agentes relacionados con una temática determinada para fomentar un avance en cuestiones de investigación e innovación. En este sentido existen convocatorias tanto nacionales como internacionales para la creación de redes temáticas en áreas de especial interés. Como ejemplo, en (Sócrates, 2013) se describe la visión de la comisión europea sobre las redes temáticas. Los miembros que forman parte de las redes temáticas

suelen ser centros de investigación, universidades, facultades o departamentos. Debido a que todos los miembros deben compartir actividades o intereses, es común que las redes temáticas no sean demasiado generalistas y se definan en disciplinas de ámbito o aplicación claramente definidas. Aunque la creación de comunidades en redes temáticas es útil en entornos de investigación, la orientación de una red de estas características al aprendizaje tiene unos retos distintos que superar, en tanto está orientada a un público con menos conocimientos. De hecho, para que esto fuera posible al menos se deberían llevar a buen puerto una serie de hipótesis iniciales.

- **Hipótesis 1.** Una red temática puede ser una herramienta importante para el aprendizaje a través de redes telemáticas. La red temática puede difundir los recursos ofrecidos por la comunidad a través de los medios que tenga disponibles sin que esto afecte a la credibilidad de la misma.
- **Hipótesis 2.** Una red temática abierta con fines de formación mantendrá en el tiempo la aportación de sus miembros creando nuevas relaciones y realimentando la misma red. Esta cuestión es importante ya que muchas redes temáticas con el paso de unos pocos años se estancan en contenidos e interés.
- **Hipótesis 3.** La red temática fomentará los encuentros y discusiones entre miembros y no miembros para favorecer la generación de nuevo conocimiento accesible a la ciudadanía sobre la temática de interés.
- **Hipótesis 4.** La información de la comunidad es abierta y gratuita a todos los usuarios, pero sólo los miembros de la red pueden generarla. Como esto es crítico para la excelencia de la red, se define un sistema de control interno de calidad de sus publicaciones.
- **Hipótesis 5.** La apertura de la red temática orientada al aprendizaje facilitará la adopción de la misma como centro de referencia de recursos de aprendizaje para la disciplina tratada, ya sea desde un punto de vista científico o para la educación de la ciudadanía.

Para verificar estas hipótesis en una red temática orientada al aprendizaje, en el año 1999 nace en la Universidad Politécnica de Madrid la Red Temática de Criptografía y Seguridad de la Información Criptored (Criptored, 2013a), una comunidad virtual de cooperación en temas relacionados con la seguridad informática, prestando especial interés en solventar algunos de los problemas clásicos de las redes temáticas: abandono de la red por parte de sus miembros, contenidos exclusivos de investigación y alejados de cuestiones académicas, pocos miembros productores de información, escasa difusión del contenido y poca relación entre los miembros de la red (productores y consumidores); así como resolver algunos retos:

- Abrir las redes temáticas a un público más generalizado, evitando ser rígidas a un público concreto (grupos de investigación).
- Verificar que el contenido es interesante para un público que no tiene porqué pertenecer a la red y resaltar que el interés en dicha red se mantiene a lo largo del tiempo.
- Establecer criterios para gestionar la calidad de los contenidos y la medición del grado de utilización y utilidad de la red temática.

- Ser generador de nuevas iniciativas que permitan realimentar la red temática.

## Criptored y la educación global. Resultados de la experiencia

### Diseño y objetivos. Decisiones

El 19 de julio de 1999 se ponen los primeros cimientos para crear una red social orientada a la difusión de la temática de la seguridad de la información. Entre sus objetivos destaca la creación de un espacio virtual y común para las universidades e institutos de investigación de países iberoamericanos, a través del cual sea posible intercambiar todo tipo de información docente en el amplio ámbito de la seguridad de la información, que conduzca a una plena integración académica entre las entidades y miembros de dicha red. Es menester indicar que en aquel entonces no existían las redes sociales que hoy conocemos y que, por tanto, Criptored como decana de las redes temáticas es un claro caso de éxito de innovación educativa.

En este sentido, la red temática se articuló considerando una serie de cuestiones: estructuración docente de la información, gestión de la calidad de los contenidos, esquema de difusión de la información y fomento de eventos, discusiones e interacciones entre miembros y no miembros de la comunidad.

#### a) Estructuración docente de la información

La red temática actúa como un repositorio Web de información subida por sus miembros, cuya aprobación dependerá del sistema de gestión de calidad habilitado. Los documentos son clasificados por temática. La página web de la red temática se estructura de tal forma que se simplifique el acceso a los elementos más importantes de la red (miembros, documentos, formación multimedia, MOOC e información de eventos). No es necesario ningún tipo de autenticación para navegar o descargar información en la red temática (véase gráfico 2).

The screenshot shows the homepage of the Criptored website. The header is yellow with the Criptored logo on the left, the title 'red temática de criptografía y seguridad de la información' in the center, and the Politécnica logo on the right. Below the header, there is a sidebar on the left titled 'CONTENIDOS' with a list of links. The main content area has a 'Noticias del Mes' section with two news items, each with a date and a 'Leer más...' link. To the right of the news, there are two boxes for upcoming congresses: 'CIBSI 7a edición 2013' and '2º TIBETS 2013'. At the bottom right, there is a calendar for March 2013.

Gráfico n.2. Página Web de la red temática Criptored



### b) Gestión de la calidad de los contenidos

Una red temática orientada al aprendizaje tiene el reto de generalizar la información a un público heterogéneo sin perder calidad ni excelencia; del mismo modo, es necesario decidir si cualquier persona puede publicar en la red. En el caso de Criptored se opta por permitir el alta gratuita como miembros de la red sólo a profesores universitarios, investigadores y profesionales de la seguridad informática. Sólo estos miembros pueden proponer nuevo material para la red, si bien cualquier usuario de Internet podrá leerlo. Esto podría ser un inconveniente pero se piensa que es la mejor opción para mantener la calidad y que la red temática pueda abrirse al público global. Así, la gestión de la calidad se basa en un sistema de confianza apoyado por la reputación de sus miembros y en ciertos casos asesoramiento de los mismos, si bien todo se publica siempre bajo la responsabilidad de su autor.

### c) Esquema de difusión y compartición de la información

La red temática está evolucionando continuamente para adaptarse a nuevos mecanismos de difusión y compartición de sus recursos a la globalidad de la ciudadanía. En sus inicios, opciones que todavía se mantienen, sólo era posible descubrir nuevo material en la red navegando por la página web o mediante un correo mensual de novedades enviado a los miembros de dicha red. En la actualidad, e independientemente de la publicidad que terceros puedan hacer de estas noticias, la publicación Web y el envío mensual de correos se complementa con la notificación de nueva información mediante redes sociales (Facebook y Twitter) y RSS. Estos mecanismos actuales permiten llegar a un público más heterogéneo, permitiendo diferenciar miembros de la red de un público más genérico que podría acceder al contenido vía Twitter o RSS.

### d) Generación de nuevo contenido basado en interacciones de miembros y no miembros de la red

La red temática se diseña de forma que periódicamente informe sobre congresos, seminarios, conferencias o nueva documentación aportada relacionados con la temática de la red, de forma que miembros y no miembros encuentren un servicio de referencia al que consultar. Para que la red no sea un elemento de uso esporádico (sólo descargar documentos), es importante que muestre información de interés para su entorno y que ésta cambie relativamente rápido (diferente cada semana), simplificando su consulta a profesionales e investigadores del sector.

Un estudio con mayor profundidad sobre el diseño, gestión y mantenimiento de esta red temática se encuentra en el documento “Proyecto de actualización del servidor web de la red temática de criptografía y seguridad de la información Criptored” (Ramíó, 2013). En el próximo apartado se observa cómo la interacción con miembros y empresas de la red da lugar a proyectos derivados de interés para la red que, a su vez, son útiles para generar nuevo material publicable en la misma.

## Impacto y difusión. Proyectos derivados

La red refleja un impacto significativo en universidades, centros de investigación y empresas TIC en España e Iberoamérica. Algunas de las cifras más significativas a diciembre de 2012 (Criptored, 2013b) son:

- 243 universidades, centros de investigación y asociaciones de 22 países.
- 925 miembros de la red, 1.449 seguidores en Twitter y 155 en Facebook.
- 33.700 referencias en Google. Otros sitios de referencia enlazan material de la red como es el caso del Instituto Nacional de Tecnologías de la Información.
- 448 documentos para libre descarga, 14 libros electrónicos y 102 vídeos.
- Datos anuales del año 2012: 488 GB de tráfico, 303.093 documentos servidos, 457.701 visitas.
- Más de 2.500.000 de documentos servidos en 13 años.

La apertura de la red temática a la ciudadanía y la colaboración de sus miembros ha tenido como resultado el fomento de congresos, seminarios, conferencias y diferentes iniciativas docentes de gran impacto. El resultado de estos proyectos derivados ha repercutido en nuevo material para la red en forma de artículos científicos y contenido multimedia de formación y concienciación; véase como ejemplo la sección multimedia de la red (Criptored, 2013a). Los proyectos derivados apoyados y constituidos por la red han sido:

a) **Congreso CIBSI:** 6 ediciones del Congreso Iberoamericano de Seguridad Informática (véase gráfico 3). El objetivo principal es promover y desarrollar el área de la seguridad de la información creando para ello un espacio académico y tecnológico que facilite el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación y el desarrollo, con 193 publicaciones científicas (Cibsi, 2013).





b) **Congreso TIBETS:** Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (véase gráfico 4). En su primera edición en 2011 se publican 18 ponencias (Cibsi, 2013).



Gráfico n.4. Última edición de taller TIBETS.

c) **Cátedra universidad-empresa UPM Applus+:** Desde 2007 a 2010 (Applus, 2013) con acciones de difusión y concienciación en el marco de Criptored. Las más significativas son:

- 5 Jornadas anuales de DISI, Día Internacional de la Seguridad de la Información, con 36 ponencias y 5 mesas redondas, y la asistencia de investigadores de nivel mundial como Martin Hellman, Taher Elgamal o Radia Perlman.
- 5 Seminarios especializados con expertos españoles: 21 conferencias y 4 mesas redondas.

d) **Conferencias anuales TASSI:** Temas Avanzados en Seguridad y Sociedad de la Información, desde el año 2005 con 60 conferencias donde destacan ponentes de universidades, empresas del sector TIC, organismos oficiales o fuerzas y cuerpos de seguridad del estado (Tassi, 2013). Muchas de estas conferencias de la cátedra y TASSI han sido grabadas en vídeo y publicadas en la red temática (Criptored, 2013c).

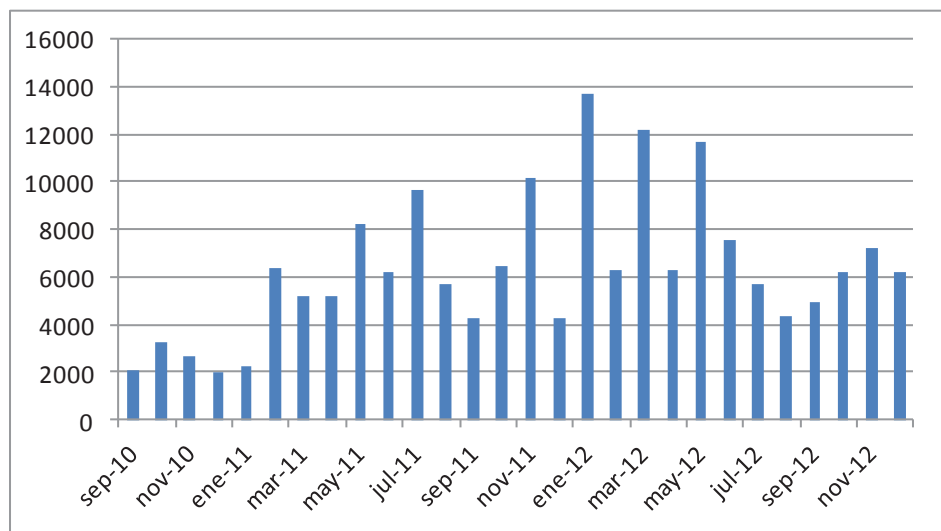
e) **Proyecto Intypedia - Criptored** (con la empresa GMV desde septiembre de 2010 a julio 2012). Acciones de difusión y concienciación mediante la Enciclopedia Visual de la Seguridad de la Información Intypedia (Intypedia, 2013a). El proyecto difunde a través de avatares conocimientos sobre seguridad de la información mediante lecciones en vídeo desarrolladas por destacados expertos, usando un lenguaje accesible por un amplio público, gráfico 5. La enciclopedia abarca temas tan variados como la criptografía, la seguridad en redes, la gestión de riesgos, etc. Se publican 14 lecciones en español e inglés. Como continuación del proyecto, en el último trimestre de 2012 y con el patrocinio de la Agencia de Protección de Datos de la Comunidad de Madrid, se publican tres nuevas

lecciones entre noviembre de 2012 y enero de 2013. En poco más de dos años de vida se han alcanzado unas cifras (Intypedia, 2013b) muy importantes: 232.786 reproducciones, más de 40.000 entradas en Google, 1.233 seguidores en Facebook y 869 seguidores en Twitter.



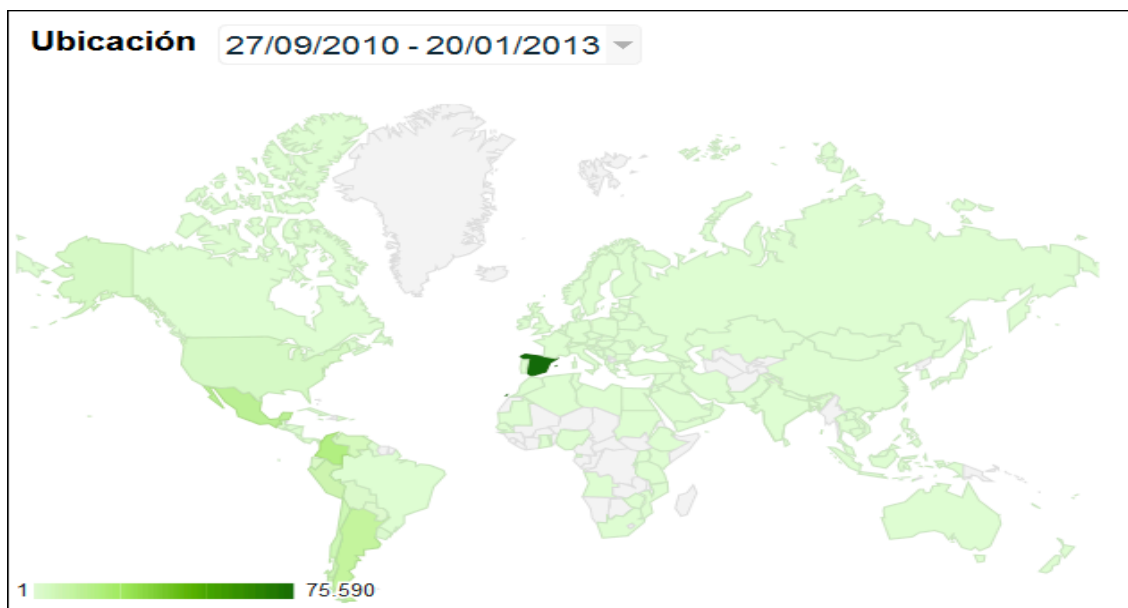
**Gráfico n.5.** Página Web del proyecto intypedia.

El gráfico 6 detalla el número de descargas de documentos asociados a las lecciones del proyecto intypedia a 1 de Enero de 2013 (176.264). Estos documentos son, en formato pdf, un guión, diapositivas de apoyo y ejercicios de autoevaluación.

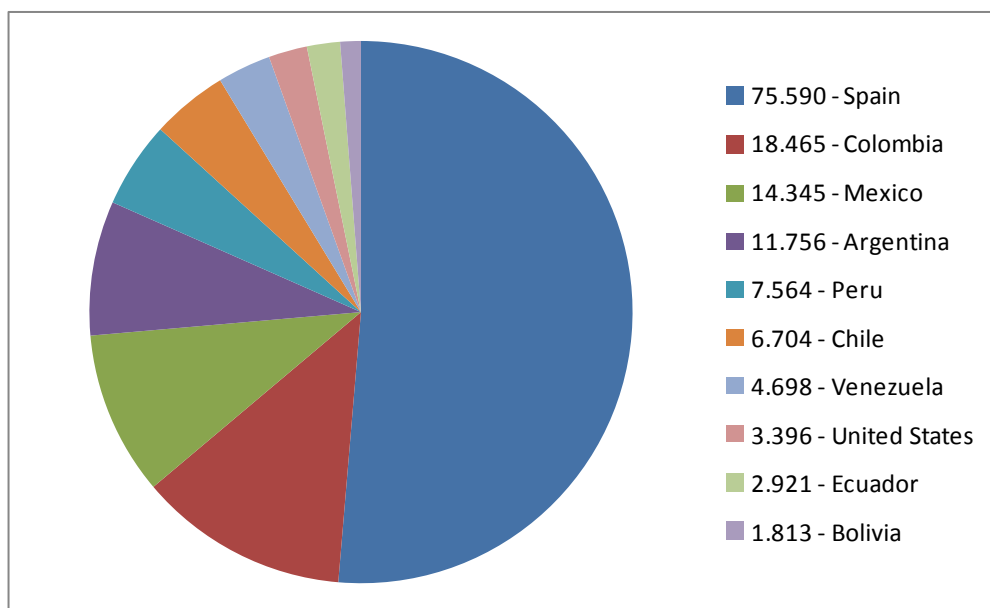


**Gráfico n.6.** Estadísticas de descargas de documentos pdf asociados a lecciones

Por último, el gráfico 7 y el gráfico 8 muestran una captura de Google Analytics para el sitio Web intypedia.com, donde destacan la gran cantidad de países en los cuales se siguen las lecciones de esta Enciclopedia. Es menester indicar que estos datos de acceso y tráfico corresponden sólo al sitio Web indicado y no a la visualización de los vídeos desde el canal YouTube, que obviamente son mayores.



**Gráfico n.7.** Accesos al servidor Web de Intypedia. 163.304 visitas - 137 países



**Gráfico n.8.** Distribución de visitas por países (los más significativos)

f) [Aula Virtual de Criptografía y Seguridad de la Información Crypt4you](#). Plataforma para la publicación de Massive Open Online Course (MOOCs) dentro de Criptored, un nuevo formato de enseñanza masiva, online y gratuita, gráfico 9.

En la actualidad existe una demanda importante de formación técnica especializada en aspectos relacionados con la protección de comunicaciones digitales. En ocasiones es suficiente con propuestas que simplifiquen aspectos complejos y los muestren con un lenguaje accesible a un gran público heterogéneo, como es el caso de la experiencia educativa Intypedia; en otros casos es necesaria una formación extensa y detallada de una manera guiada. En este sentido los MOOC son una excelente opción a explotar. Conocida la evolución de los paradigmas en aprendizaje y las necesidades concretas de

conocimiento en los países de lengua hispanohablante<sup>1</sup> relativo a temas de seguridad de la información, se publica en marzo de 2012 en la Universidad Politécnica de Madrid el proyecto de Aula Virtual de la Seguridad de la Información Crypt4you. El objetivo de esta plataforma es la publicación de cursos gratuitos online en formato MOOC sobre criptografía y seguridad de la información, como una nueva oferta educativa dentro de la Red Temática de Criptografía y Seguridad de la Información Criptored.

En 10 meses, entre marzo 2012 y enero de 2013, (gráfico 10), se publica completo el curso El algoritmo RSA (Crypt4you, 2013a) formado por 10 lecciones con la siguiente repercusión al 31/12/2012: 106.266 lecturas (Crypt4you, 2013b), 10.800 entradas en Google, 516 seguidores en Facebook y 412 en Twitter.



The image shows a screenshot of the Crypt4you website. At the top, there is a navigation bar with various icons and labels like 'Paper', 'FCOE', '7PM', 'TRABAJO FUTURO', 'Programas', 'DIARIO', 'CONSULTA DIARIA', 'Musica', 'Ingles', 'CIII', 'Arduino', 'Presentaciones', and 'LATEX'. Below this is the main header with the text 'Crypt4you. Aula Virtual' and social media icons for Twitter, Facebook, and YouTube. The text 'Aula Virtual de Criptografía y Seguridad de la información Crypt4you' and 'Universidad Politécnica de Madrid' is also present. Below the header, there is a video player showing a presentation titled 'Presentación del Aula Virtual Crypt4you'. The video player shows a slide with the Crypt4you logo and the text 'Aula Virtual de Seguridad de la Información' and 'Un proyecto de la Red Temática Criptored Universidad Politécnica de Madrid - España'. To the right of the video player, there is a text block describing the project: 'Crypt4you es un nuevo formato de enseñanza en seguridad de la información, masiva, online y gratuita. Un MOOC, Massive Open Online Course, que nace en marzo de 2012 dentro la Red Temática de Criptografía y Seguridad de la Información Criptored, en la Universidad Politécnica de Madrid, España. Cada nuevo tema que se ofrezca en estos cursos estará compuesto por un conjunto de lecciones que se publicarán en el sitio Web del proyecto cada quince días, siendo sus autores investigadores y profesores miembros de esta red temática. El objetivo de Crypt4you es convertirse en el Aula Virtual de referencia de seguridad de la información en lengua hispana. Para solucionar cualquier duda, por favor consulta las FAQs (Frequently Asked Questions) o contacta con nosotros por correo electrónico.'

**En portada**

**4/01/2013. MOOC El algoritmo RSA. Lección 10: Ataque por paradoja del cumpleaños**

En esta última lección del curso se estudia el ataque a una clave RSA mediante la paradoja del cumpleaños. Lo interesante del mismo es que nos permite encontrar la clave privada o una clave privada pareja de la víctima, sin necesidad de factorizar el módulo y contando para ello sólo con datos públicos de la misma. Ni siquiera es necesario capturar un criptograma como en el ataque por cifrado cíclico visto en la lección anterior.

**Gráfico n.9. Massive Open Online Course – Crypt4you**

Página o título de la lección	Subida	Acumulado
Página principal: Portada	15/03/12	43.538
Lección RSA 00: Introducción al curso	15/03/12	26.583
Lección RSA 01: Los principios del algoritmo RSA	15/03/12	15.175
Lección RSA 02: Valores de diseño de las claves	30/03/12	5.304
Lección RSA 03: Cifrado de números y mensajes	13/04/12	4.745
Lección RSA 04: Claves privadas y públicas parejas	04/05/12	4.667
Lección RSA 05: Mensajes no cifrables	21/05/12	3.816
Lección RSA 06: RSA y el Teorema Chino del Resto	13/06/12	3.363
Lección RSA 07: Generación de Claves con OpenSSL	27/07/12	4.074
Lección RSA 08: Ataque por factorización	09/10/12	3.183
Lección RSA 09: Ataque por cifrado cíclico	16/11/12	2.046
Lección RSA 10: Ataque por paradoja del cumpleaños	04/01/13	1.306
Total accesos curso El Algoritmo RSA en 10 meses		<b>113.275</b>

**Gráfico 10. Accesos a Crypt4you del 15 de marzo de 2012 al 15 de enero de 2013**

Todos estos proyectos tienen como consecuencia que la producción multimedia de los proyectos asociados a Criptored al 31/12/2012 supere las 700.000 reproducciones, casi un 20% del total de canal YouTube de la UPM (Criptored, 2013d).

## Conclusiones

La red temática Criptored surgió del interés en ofrecer un espacio común a las universidades e institutos de investigación de los países iberoamericanos a través del cual fuera posible intercambiar todo tipo de información docente en el ámbito de la seguridad de la información, que condujera a una plena integración académica entre las entidades y miembros de dicha red. Dado el incipiente interés que en 1999 se observaba en diversos sectores de la sociedad sobre conceptos relacionados con esta seguridad, se vio interesante abrir la red temática a un público heterogéneo, no exclusivamente académico, lo cual presentó una serie de dudas y retos en lo que a la continuidad de la red se refería, especialmente en la calidad de su información y su excelencia.

Para solventar los retos de calidad y excelencia en un entorno abierto, se diseñó una política de aceptación de miembros en la red y una política de gestión de la calidad de los trabajos basada en un sistema de reputación y asesoramiento. Los miembros de la red (docentes, investigadores y profesionales del sector) pueden publicar sus trabajos o aquellos tutelados por ellos, y todo usuario de Internet pueden leerlos. Esta decisión equilibró la necesidad de que el material sea de calidad y que cualquiera pudiese acceder al mismo.

Un punto significativo en la continuidad y la evolución de la red ha sido la interacción entre miembros y no miembros y acciones dirigidas para convertir Criptored en un centro de referencia de información y formación de seguridad informática en España e Iberoamérica. En esta tarea, ha tenido una gran importancia la apertura de la red a colaboraciones empresariales y la publicación de noticias variadas de interés (no exclusivamente documentos o libros). El gran éxito de la red ha consistido en vincular a todos los interesados en esta temática en el desarrollo de nuevas iniciativas docentes, académicas y divulgativas (CIBSI, TIBETS, DISI, TASSI, Intypedia, Crypt4you) que han permitido realimentar con contenidos la red y evolucionarla con el paso de los años.

Puede afirmarse, después de 13 años de experiencia, que verificadas las hipótesis formuladas en el artículo, los mecanismos diseñados son aptos para la adaptación de una red temática hacia al aprendizaje global y es factible construir este tipo de redes orientadas a un público no especialmente técnico ni formado sin perder calidad ni excelencia, satisfaciendo necesidades docentes, investigadoras y divulgativas.

## Referencias bibliográficas

- Applus (2013). *Cátedra UPM Applus+ CAPSDESI*. Recuperado de <http://www.capsdesi.upm.es/>
- Boyd, D. y Ellison, N (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13(1), article 11. Recuperado de <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>

- Criptored (2013a). *Red Temática de Criptografía y Seguridad de la Información Criptored*. Recuperado de <http://www.criptored.upm.es/>
- Criptored (2013b). *Estadísticas publicadas de Criptored*. Recuperado de <http://www.criptored.upm.es/paginas/estadisticas.htm>
- Criptored (2013c). *Sección multimedia de la Red Temática Criptored*. Recuperado de <http://www.criptored.upm.es/multimedia/index.php>
- Criptored (2013d). *Reproducciones multimedia en Criptored*. Recuperado de [http://www.lpsi.eui.upm.es/~jramio/curriculum/Reproducciones\\_video\\_JRA\\_en\\_Canal\\_YouTube\\_UPM\\_octubre\\_2012.pdf](http://www.lpsi.eui.upm.es/~jramio/curriculum/Reproducciones_video_JRA_en_Canal_YouTube_UPM_octubre_2012.pdf)
- Cibsi (2013). *Congreso Iberoamericano de Seguridad Informática CIBSI*. Recuperado de <http://www.criptored.upm.es/cibsi/cibsi.htm>
- Crypt4you (2013a). *Aula Virtual MOOC Crypt4you El algoritmo RSA*. Recuperado de <http://www.criptored.upm.es/crypt4you/portada.html>
- Crypt4you (2013b). *Estadísticas MOOC Crypt4you*. Recuperado de <http://www.criptored.upm.es/paginas/crypt4youmensual.htm>
- Intypedia (2013a). *Enciclopedia Visual de la Seguridad de la información*. Recuperado de <http://www.intypedia.com/>
- Intypedia (2013b). *Estadísticas Intypedia*. Recuperado de <http://www.criptored.upm.es/paginas/intypediamensual.htm>
- Jódar, F. (2013). Profesor Youtube. *Revista Muy Interesante vol. nº380*, 70-74
- Ramió, J. (2013). *Proyecto de actualización del servidor web de la red temática de criptografía y seguridad de la información Criptored*, Trabajo Fin de Máster, 2011, Campus Sur UPM, Madrid. Recuperado de [http://www.criptored.upm.es/guiateoria/gt\\_m001a1.htm](http://www.criptored.upm.es/guiateoria/gt_m001a1.htm)
- Rheingold, H. (1993). *The virtual Community*. Recuperado de <http://www.rheingold.com/vc/book/index.html>
- Sócrates (2013). *Erasmus Thematic Networks (Socrates). Education, audiovisual & culture executive agency. European Comission*. Recuperado de [http://eacea.ec.europa.eu/static/en/overview/ThemNetwks\\_overview.htm](http://eacea.ec.europa.eu/static/en/overview/ThemNetwks_overview.htm)
- Tassi (2013). *Conferencias UPM TASSI*. Recuperado de <http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm>

Artículo concluido el 14 de Marzo de 2013

Muñoz Muñoz, A.; Ramió Aguirre, J. (2014). Criptored y las redes temáticas orientadas a la educación global. *REDU: Revista de Docencia Universitaria*, 12 (1), pp. 427-441.

Publicado en <http://red-u.net>

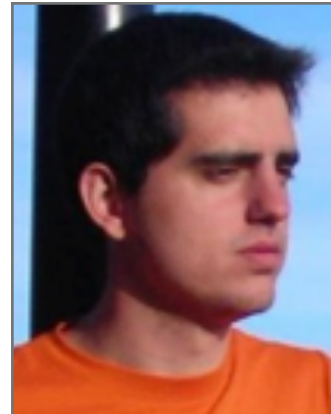
<sup>1</sup> Esta necesidad es observada gracias a la Red Temática de Criptografía y Seguridad de la Información Criptored, que desde la Universidad Politécnica de Madrid lleva más de <sup>13</sup> años difundiendo información a países principalmente hispanohablantes.



## ***Alfonso Muñoz Muñoz***

***Universidad Politécnica de Madrid  
Escuela Universitaria de Ingeniería Técnica de Telecomunicación  
Departamento de Ingeniería y Arquitecturas Telemáticas***

***Mail: amunoz@diatel.upm.es***



Doctor de Telecomunicaciones por la Universidad Politécnica de Madrid. Especialista en protección de datos digitales y diseño de sistemas seguros (criptografía, esteganografía, dpi, etc.). Ha publicado más de 20 artículos en revistas y congresos científicos de alto impacto (revisión ciega por pares) en el campo de la seguridad informática, y ha trabajado en proyectos con organismos europeos, ministerios y multinacionales. Su trabajo de investigador lo combina con su faceta de divulgación. Algún ejemplo destacable es la creación y dirección técnica de Intypedia, creación del primer MOOC en español sobre seguridad de la información Crypt4you, artículos de divulgación en revistas o blogs del sector o la participación en conferencias de seguridad informática y hacking.

## ***Jorge Ramió Aguirre***

***Universidad Politécnica de Madrid  
Escuela Universitaria de Informática  
Departamento de Lenguajes y sistemas***

***Mail: jramio@eui.upm.es***



Profesor Titular de la Universidad Politécnica de Madrid. Desde el año 1994 imparte diversas asignaturas relacionadas con la seguridad y criptografía. Entre sus facetas destaca su interés por la difusión de la seguridad informática en Iberoamérica. Autor del libro electrónico de Seguridad Informática y Criptografía en 2006, de libre distribución en Internet y con más de 120.000 descargas, creador en 1999 de la Red Temática de Criptografía y Seguridad de la Información Cryptedored, organización de los congresos iberoamericanos CIBSI y TIBETS, creador y director de la cátedra UPM Applus+ de seguridad, creación y dirección de la Enciclopedia de la Seguridad de la Información Intypedia y del primer MOOC en español sobre seguridad de la información Crypt4you, participación como profesor invitado en cursos de posgrado en España y países de Latinoamérica.